BEC-FRAUDE, GEDRAG ALS SLEUTEL TOT BESCHERMING

Steeds meer organisaties slaan de weg van digitalisering in. Dat biedt grote kansen, maar brengt ook risico's met zich mee. SRA wil een inhoudelijke bijdrage leveren aan het versterken van uw kantoor en de relatie met uw klanten die deze transitie doormaken. Daarom hebben wij het achterliggende jaar een serie artikelen gepubliceerd van de hand van Northwave, een gerenommeerde partij op het gebied van integrale informatiebeveiliging. In deze editie van de SRAadviseur de (vooralsnog) laatste bijdrage in deze reeks.

Bij BEC-fraude wordt een medewerker of medewerkster die betalingen mag verrichten, misleid om een valse factuur te betalen of ongeoorloofd van de bedrijfsrekening over te schrijven.

Een 'vreemd' verzoek

Het is donderdagmiddag 16.00 uur bij accountantskantoor Precisie. Boudewijn, een medewerker die gemachtigd is om betalingen te doen, ontvangt van vennoot Noor per e-mail het verzoek om twee facturen aan een IT-leverancier te betalen. Hij geeft aan dit morgenvroeg te doen en ontvangt bevestiging van Noor dat dit akkoord is. Vervolgens zet hij de volgende dag de betaling in gang, maar het valt hem op dat de bankrekening-gegevens gewijzigd zijn. Noor geeft opnieuw per mail aan dat dit klopt en Boudewijn neemt contact op met de bank om de gegevens te wijzigen en alsnog de betaling te kunnen doen. Na enige tijd belt de leverancier boos op, hij heeft helemaal nooit zijn geld ontvangen. Wat is hier gebeurd?

SCHADE

Inge van der Beijl, director Safe Behaviour & Training Northwave: "Het bedrijf is slachtoffer geworden van BEC-fraude. BEC-fraude staat voor Business E-mail Compromise-fraude en is een geavanceerde vorm van cybercriminaliteit die diverse varianten kent (o.a. de zogeheten CEO-fraude)." BEC-fraude komt steeds vaker voor en zorgt voor steeds meer slachtoffers en steeds hogere bedragen aan schade. BEC-fraude behoort zelfs al tot de top-3 vormen van cybercriminaliteit in termen van financiële schade. Van der Beijl: "In Nederland werd bijvoorbeeld in 2018 Pathé slachtoffer van CEO-fraude, wat een verlies van € 19 miljoen tot gevolg had!"

CEO-FRAUDE

De cybercrimineel weet in dit geval in de haarvaten van de organisatie te kruipen, de financiële processen te doorgronden en gebruik te maken van het natuurlijk gedrag van medewerkers. Het gaat hier om een 'regulier' financieel verzoek vanuit de leidinggevende (autoriteit) onder hoge tijdsdruk (urgentie), een verzoek waar weinig mensen nee tegen zullen zeggen. Naast deze CEO-fraude, zijn er ook andere vormen van BEC-fraude zoals het verzoek tot het betalen van valse facturen of het naar klanten verzenden van valse facturen uit naam van een medewerker, aldus Van der Beijl.

De hacker

Het is hacker Bart eerder die week gelukt om de controle over de mailbox van Noor te krijgen. Hij heeft een phishing e-mail gestuurd met hierin een bijlage die alleen via een inlogscherm gelezen kon worden. Noor wilde de bijlage graag inzien en heeft automatisch haar inloggegevens gedeeld. Noor gaf hiermee hacker Bart de gelegenheid om haar mailbox over te nemen. Hierdoor heeft de hacker goed kunnen zien hoe het betaalverkeer in de organisatie normaal verloopt en wat de 'tone of voice' is in de mails. In een reguliere mail met facturen vraagt de hacker uit naam van Noor aan Boudewijn om het bedrag over te maken naar een aangepast bankrekeningnummer. Hierbij oefent de hacker veel druk uit op Boudewijn om het bedrag snel over te maken en geen lastige vragen te stellen. Boudewijn heeft uiteindelijk alles in werking gezet om het bedrag over te maken naar de verkeerde rekening.

CYBER(ON)VEILIG GEDRAG MAAKT HET VERSCHIL

Van der Beijl: "Bij deze vorm van fraude maakt de crimineel handig gebruik van de mens als zwakste schakel. Gewoontes en nieuwsgierigheid maken dat Noor haar inloggegevens weggeeft. Tijdsdruk, de wens om te helpen en het autoriteitsprincipe maken dat Boudewijn alles in werking stelt om het bedrag over te maken. In het voorbeeld wordt duidelijk dat de sleutel tot het beschermen van je organisatie bij alle medewerkers ligt, van directie tot financieel medewerker. Hierbij is het belangrijk dat medewerkers zich niet alleen bewust zijn van de risico's die zij lopen, maar er ook naar handelen. Het gaat om cyberveilig gedrag."

Valse factuur

Boudewijn was in eerste instantie scherp en zag dat de betalingsgegevens op de factuur veranderd waren. Hij heeft Noor hierop aangesproken. Uit naam van Noor heeft de cybercrimineel de gemanipuleerde factuur, tot grote frustratie van Boudewijn, er uiteindelijk doorheen gedrukt. Deze BEC-fraude is aan het licht gekomen toen Noor werd aangesproken, door de manager van Boudewijn, op haar gedrag richting Boudewijn, en doordat de echte leverancier contact opnam met de vraag waar zijn betaling bleef.

HOE HERKEN JE BEC-FRAUDE?

Cyberveilig gedrag begint met bewustzijn en begrijpen. Van der Beijl tipt aan welke signalen je mogelijke BEC-fraude kunt herkennen:

- Het gaat om een spoedbetaling of je wordt onder druk gezet.
- Je wordt in vertrouwen genomen of gevraagd het normale proces even niet te volgen.
- Het zijn onverwachte of ongevraagde vreemde verzoeken van een leidinggevende (rechtstreeks van bijvoorbeeld de vennoot of directeur).

WAT ZIJN JE HANDELINGSPERSPECTIEVEN?

Cyberveilig gedrag gaat verder dan alleen bewustzijn en begrijpen, zegt Van der Beijl. “Medewerkers moeten ook kunnen en willen handelen. Daarom is ondersteuning vanuit de organisatie noodzakelijk en kun je niet volstaan met een eenmalige activiteit als het gaat om ‘awareness’.” De volgende handelingsperspectieven dienen onderdeel van de bedrijfsprocessen en bedrijfscultuur te worden:

- Bij gewijzigde factuurgegevens, spoedbetalingen of vreemde verzoeken, altijd controleren door te bellen (richt een proces voor het vierogenprincipe in).
- Laat je niet onder druk zetten en volg altijd het afgesproken en normale proces. Wees extra alert op verzoeken aan het einde van de dag, week of maand.
- Accepteer niet zomaar onverwachte of ongevraagde rechtstreekse verzoeken van een leidinggevende (bijvoorbeeld de vennoot of directeur).

WAAROM IS DIT VOOR U ALS ACCOUNTANTSKANTOOR BELANGRIJK?

Vanuit de beroepsregels geldt dat een accountant in ieder geval de verantwoordelijkheid heeft om fraude en corruptie te signaleren. BEC-fraude valt hieronder. Onderzoek van securitybedrijf Mimecast laat zien dat er in Q3 van 2019 269% meer BEC-aanvallen zijn waargenomen ten opzichte van het voorgaande kwartaal. E-mailbeveiligingssystemen zijn simpelweg niet effectief genoeg. Er komen duizenden schadelijke e-mails in de mailboxen van de medewerkers terecht. Zij staan onder grote druk om zelf veilige keuzes te maken. Cybercriminelen zijn telkens op zoek naar nieuwe manieren om traditionele beveiligingssystemen te omzeilen en gebruikers te misleiden. Cyberveilig gedrag is dus alleen te bereiken door een continu ‘Cyber Safe Behaviour-programma’. Alleen op deze manier worden de medewerkers ‘first line of defense’ in plaats van ‘last line of defense’. Aarzel niet om hierbij zonodig professionele ondersteuning in te roepen, de risico’s zijn er groot genoeg voor.

MEER INFORMATIE

Kijk op www.sra.nl voor meer informatie over cybersecurity of mail uw vraag naar automatisering@sra.nl.

> “INGE VAN DER BEIJL
> **BIJ BEC-FRAUDE WORDT EEN MEDEWERKER DIE BETALINGEN VERRICHT, MISLEID OM EEN VALSE FACTUUR TE BETALEN.”**